

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,
Plaintiff,
v.
JOSEPH SULLIVAN,
Defendant.

Case No. [20-cr-00337-WHO-1](#)

**ORDER ON MOTIONS IN LIMINE,
MOTIONS TO EXCLUDE, AND
OBJECTIONS TO EXHIBITS**

Re: Dkt. Nos. 137, 138, 139, 146, 148

Defendant Joseph Sullivan is charged with obstructing a federal proceeding in violation of 18 U.S.C. § 1505 and misprision of a felony in violation of 18 U.S.C. § 4, arising out of his alleged efforts to cover up a data breach suffered by Uber Technologies, Inc. (“Uber”). Before me are several pretrial motions by Sullivan and the government—motions in limine and two motions to exclude expert witnesses—along with their objections to certain exhibits. My decisions, subject to change depending on the presentations at trial, are detailed below.

BACKGROUND

This case arises from a data breach at Uber in November 2016 (“the 2016 Incident”), when the government alleges that hackers gained unauthorized access to the company’s data containing personally identifiable information of Uber users and drivers, including appropriately 600,000 drivers’ license numbers. Superseding Indictment (“SI”) [Dkt. No. 71] ¶ 4. On September 3, 2020, a grand jury indicted Sullivan (who was Uber’s Chief Security Officer at the time of the 2016 Incident) on charges of obstructing the Federal Trade Commission (“FTC’s”) investigation into Uber’s data security program and practices, in violation of section 1505, and misprision of a felony, in violation of section 4. Dkt. No. 13. The Superseding Indictment added three wire fraud counts, alleging that Sullivan violated 18 U.S.C. § 1343 when scheming to defraud Uber drivers.

SI ¶¶ 15-16.

Sullivan moved to dismiss the wire fraud counts on April 11, 2022. Dkt. No. 107. I denied the motion but held that the charges could not proceed on an omission theory because the Superseding Indictment failed to state that Sullivan owed an independent duty to disclose the data breach to the allegedly defrauded party: Uber drivers. Order Denying Mot. to Dismiss (“MTD Order”) [Dkt. No. 129] 1:22-28. The Superseding Indictment cited California Civil Code section 1798.82(a), which imposes a duty to disclose a data breach upon a “person or business that conducts business in California, and that owns or licenses computerized data that includes personal information.” SI ¶ 8. I held that although it appeared that section 1798.82(a) imposed a duty upon *Uber* to disclose the breach, the SI did not allege that Sullivan owned or licensed the data that was breached, as required to establish a duty under the statutory language. MTD Order at 12:12-13:13.

The government later moved to dismiss the wire fraud counts, which was granted on August 2, 2022. That leaves only the section 1505 and section 4 charges. *See* Dkt. Nos. 133, 134.

The elements of those crimes help frame the issues presented in the pretrial motions. For a jury to find Sullivan guilty of section 1505, the government must prove beyond a reasonable doubt: (1) the existence of a proceeding pending before a department or agency of the United States; (2) Sullivan’s awareness of the pending proceeding; and (3) that Sullivan intentionally endeavored corruptly to influence, obstruct, or impede the pending proceeding. *See United States v. Price*, 951 F.2d 1028, 1031 (9th Cir. 1991). To convict Sullivan of violating section 4, the government must prove beyond a reasonable doubt that: (1) a federal felony was committed; (2) Sullivan had knowledge of the commission of that felony; (3) Sullivan had knowledge that the conduct was a federal felony; (4) Sullivan failed to notify a federal authority as soon as possible; and (5) Sullivan did an affirmative act to conceal the crime. *See United States v. Olson*, 856 F.3d 1216, 1220 (9th Cir. 2017); 9th Cir. Model Crim. Jury Instr. 24.1 (2022).

DISCUSSION

I. MOTIONS IN LIMINE

There are five motions in limine, all filed by Sullivan, seeking to exclude the following

categories of evidence. Dkt. No. 137.

A. No. 1: Evidence of hackers' guilty pleas and related documents (including plea and cooperation agreements)

Sullivan first moves to exclude evidence of the hackers' guilty pleas and related documents, including their plea agreements, under Federal Rule of Evidence 403.¹ Mot. in Limine [Dkt. No. 137] 2:1-7:14. Rule 403 allows the court to exclude relevant evidence "if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence." Fed. R. Evid. 403.

Sullivan analogizes his case to those with co-defendants and co-conspirators, where courts have excluded evidence of guilty pleas. He first points to *United States v. Smith*, 790 F.2d 789, 793 (9th Cir. 1986), where the Ninth Circuit emphasized that "evidence of a co-defendant's guilty plea may not be offered by the government and received over objection as substantive evidence of the guilt of those on trial." Mot. in Limine at 2:10-16.

He then argues that admitting evidence of the hackers' guilty pleas would cause substantial prejudice as "jurors would have to 'perform mental acrobatics' to disregard the hackers' guilty pleas as substantive evidence of Sullivan's guilt"—which could not be cured via instruction. *Id.* at 5:2-21 (citing in part *United States v. Gomez*, 617 F.3d 88, 96 (2d Cir. 2010) ("Presuming that limiting instructions were followed is inappropriate when the instructions required jurors to perform mental acrobatics."); *Sharif v. Picone*, 740 F.3d 263, 273-74 (3d Cir. 2014) (holding that the defendant's prior assault conviction should have been excluded under Rule 403 because it stemmed from the same incident underlying his 42 U.S.C. § 1983 excessive force claim and therefore posed a "particular danger" that the jury may believe the defendant had a propensity toward acting in conformity with a prior bad act)).

According to Sullivan, the risk of prejudice is "particularly great" because he is charged

¹ Sullivan asserts that if this motion is granted, "he will not attempt, on cross-examination or otherwise, to impeach the hackers with evidence of their guilty pleas or their agreements with the government." Mot. in Limine at 1:3-7.

1 with misprision regarding the same felony to which the hackers pleaded guilty: conspiracy to
 2 commit extortion involving computers in violation of 18 U.S.C. §§ 1030(a)(7)(B) and (c)(3)(A).
 3 Mot. in Limine at 5:22-26; *see also* SI ¶¶ 13-14; Angeli Decl., Ex. 2 ¶ 1, Ex. 3 ¶ 1. As stated in
 4 *Olson*, the commission of a felony is an element of a misprision charge. 856 F.3d at 1220.
 5 Sullivan contends that if the guilty pleas are admitted, “jurors will be asked to perform the
 6 impossible ‘mental acrobatics’ of ignoring the fact that the hackers have admitted committing the
 7 very felony that constitutes an element of the misprision offense.” Mot. in Limine at 6:1-3. In
 8 support, he points to a Third Circuit case describing the risk that accompanies evidence of a guilty
 9 plea to a conspiracy charge: such a plea “carries with it more potential harm to the defendant on
 10 trial because the crime by definition requires the participation of another.” *Id.* at 6:3-11 (citing
 11 *United States v. Universal Rehab. Servs. (PA), Inc.*, 205 F.3d 657, 669 (3d Cir. 2000)).

12 This case does not involve co-defendants or co-conspirators, distinguishing it from cases
 13 such as *Smith* or those discussed in *Universal Rehabilitation Services*. The risk of prejudice there
 14 is obvious: the concern is that if evidence of one co-defendant or co-conspirator’s guilty plea is
 15 introduced, the jury will import that guilt on the other—in other words, “that the defendant should
 16 be found guilty merely because of the witness’s guilty plea.” *See Universal Rehab. Servs.* at 668;
 17 *see also Baker v. United States*, 393 F.2d 604, 614 (9th Cir. 1968) (“[A] defendant is entitled to
 18 have the question of his guilt determined upon the evidence against him, not on whether a
 19 government witness or co-defendant has pleaded guilty to the same charge.”). Here, however,
 20 Sullivan is charged with an entirely separate crime than what the hackers pleaded guilty to.
 21 Moreover, the commission of a federal felony is only one element of the misprision charge. In
 22 order to convict Sullivan, the government must also prove beyond a reasonable doubt that he had
 23 knowledge of the commission of the federal felony, that he had knowledge that the conduct was a
 24 federal felony, that he failed to notify a federal authority as soon as possible, and that he did an
 25 affirmative act to conceal the crime. *See Olson*, 856 F.3d at 1220; 9th Cir. Model Crim. Jury Instr.
 26 24.1 (2022). Taken together, the concern that arises in cases with co-defendants or co-
 27 conspirators is not present here.

28 Nor does the risk of prejudice substantially outweigh the probative value of the evidence,

as required for exclusion under Rule 403. The guilty pleas are relevant to the misprision charge: they are probative of whether the 2016 Incident involved the commission of a federal felony.² The guilty pleas and accompanying plea agreements have a tendency to make a fact—whether a federal felony was committed—more or less probable than it would be without the evidence. *See* Fed. R. Evid. 401(a). The pleas and agreements are not a helpful to Mr. Sullivan but are of consequence in determining an element of the misprision charge. *See* Fed. R. Evid. 401(b). The jury instructions will make clear the multiple elements of the misprision charge and specify that the commission of a federal felony is but one of them.

This motion in limine is therefore DENIED, with the exception of the “truth-telling” provisions of the hackers’ plea agreements, which may only come in if Sullivan attacks the hackers’ credibility because of the plea agreements. *See United States v. Wallace*, 848 F.2d 1464, 1474 (9th Cir. 1988); *see also* Oppo. to Mot. in Limine at 4:23-5:6 (agreeing that the government will not elicit the truth-telling provisions unless Sullivan opens the door).

B. No. 2: Testimony or evidence concerning the legal significance of the 2016 Incident

This motion teases out two issues. The first is whether to exclude any testimony or evidence that the 2016 Incident amounted to a data breach requiring notification under California law. The second is whether testimony and evidence describing the incident as a “felony,” “ransom,” “conspiracy,” act of “extortion,” or “data breach” should be excluded.

To the first issue, Sullivan argues that any legal contention that the 2016 Incident qualified as a data breach “requiring” notification under California law is no longer relevant, given the government’s dismissal of the wire fraud counts. Mot. in Limine at 11:15-20. He notes that the remaining counts require the government to prove, among other elements, that Sullivan endeavored corruptly to influence, obstruct, or impede a pending *federal* proceeding, that he knew

² The government argues that evidence of the guilty pleas is also relevant to the hackers’ credibility. Oppo. to Mot. in Limine at 2:4-3:11. *Smith* makes clear that “under proper instruction, evidence of a guilty plea may be elicited by the prosecutor on direct examination so that the jury may assess the credibility of the witnesses the government asks them to believe.” 790 F.2d at 793 (citation omitted).

1 a *federal* felony had been committed, and that he failed to notify a *federal* authority. *See id.* at
2 9:6-10:6. Therefore, he argues, the California law is irrelevant. *Id.* at 10:2-6.

3 The government contends that California’s disclosure law is probative of Sullivan’s intent
4 and that in order to hide the 2016 Incident from the FTC and conceal the underlying felony, he
5 also had to avoid notifying Uber’s users and drivers of the breach. *See* Oppo. to Mot. in Limine at
6 6:8-17. Moreover, the government argues that there is evidence that state disclosure requirements
7 were on the minds of Sullivan and others at Uber as they responded to the 2016 Incident. *Id.* at
8 6:4-7, 7:9-12. It also asserts that given the “repeated references” to the disclosure law by
9 witnesses and documents in the case, the jury may be confused without specific evidence of the
10 disclosure requirements. *Id.* at 8:5-9.

11 There is a line between what is admissible and what is not with respect to the California
12 disclosure law. Whether the 2016 Incident required disclosure under California law is
13 inadmissible under Rule 403. The charged crimes involve a *federal* proceeding, a *federal* felony,
14 and notification of a *federal* authority. The jurors do not need to decide whether California law
15 “required” notification in this circumstance. However, evidence describing the disclosure
16 obligations generally and contemporaneous concerns about whether those obligations were
17 followed is relevant, particularly any evidence of what was told to or discussed with Sullivan, or
18 what he was aware of regarding disclosure. This evidence is probative of Sullivan’s state of mind
19 and any steps that he did or did not take to hide the 2016 Incident from the FTC or otherwise
20 conceal the underlying felony. Where specific evidence about disclosure falls on this spectrum
21 will be decided as that evidence is presented at trial.

22 Next, Sullivan moves to exclude testimony or other evidence concerning the hackers’ (or
23 any other witness’s) subjective beliefs about the legal significance of the 2016 Incident, including
24 any characterizations of the incident as “extortion,” a situation involving “ransom,” a “conspiracy
25 to illegally obtain” data, or a “felony.” Mot. in Limine at 8:2-7. Again, he argues that such
26 evidence is not relevant to Sullivan’s knowledge or intent, risks confusing the issues, and amount
27 to inadmissible legal opinions. *Id.* at 11:8-14, 12:2-19, 13:26-14:13.

28 The government asserts that these terms are used widely throughout the case; for example,

by Sullivan, others around him, and the hackers, who used words like “data breach” and “ransom” when discussing the 2016 Incident; on anticipated exhibits such as Uber’s “Data Breach Incident Response Plan” and “Breach Incident Response Playbook”; and in contemporaneous business records describing the hackers’ efforts as an “extortion attempt.” *Oppo*. at 9:2-14, 9:27-10:3.

The terms at issue are not solely used in a legal context. Lay people use words such as “data breach,” “extortion,” or “ransom,” to describe circumstances without making any legal conclusions. The use of those terms is permissible. I will make a limiting instruction, if asked, that these terms are used in their colloquial meaning and not as a term of art.

The context and manner of the hackers’ and other witnesses’ impressions of the 2016 Incident also influences whether they were relevant to what Sullivan knew or thought. Sullivan is correct that the government must prove beyond a reasonable doubt whether *he* knew, for example, that a federal felony had been committed. But if the hackers or other individuals involved in responding to the 2016 Incident described it as a “data breach,” “extortion,” or “ransom,” as the government asserts, and those representations were communicated to Sullivan, they would be relevant to what Sullivan knew or thought. *See Oppo*. at 9:2-7.³ This is certainly true if Sullivan himself used any of the terms at issue. *See id.*

As with all evidence, I will consider any specific objections raised as specific evidence is presented at trial.

C. No. 3: Brandon Glover’s statement that “[i]t was obvious to [him] then that Uber was trying to hide the second breach”

Next, Sullivan moves to exclude a portion of hacker Brandon Glover’s statement, excerpted from the government’s summary of Glover’s proffer interview and noted here in bold:

³ This is supported by the case that Sullivan relies on, *United States v. Graham*, 981 F.3d 1254 (11th Cir. 2020). In *Graham*, the Eleventh Circuit held that whether an individual who obtained a fraudulent check for the defendant believed it was a valid form of payment was not relevant because what mattered was the defendant’s knowledge or intent. 981 F.3d at 1257, 1261-62. However, the court noted that the defendant “did not present evidence that [the individual] assured him of the instruments’ authenticity,” indicating that had such evidence been proffered, the individual’s impression may be probative of what the defendant knew and thought. *Id.* at 1261-62; *see also id.* at 1262 (“[W]hat [the individual] knew and thought had no bearing on Graham’s own intent, particularly given that no evidence was ever offered to show that [the individual] expressed these thoughts to Graham.”).

After reading the news reports of the Uber data breach, Glover then realized why Uber was so willing to pay them. One of the news reports indicated that the Federal Trade Commission was already negotiating with Uber on a previous data breach. **It was obvious to Glover then that Uber was trying to hide the second breach.**

Mot. in Limine at 15:1-8 (citing Angeli Decl., Ex. 4 at 8).

Sullivan raises similar arguments as on the previous motion in limine. Glover’s “subjective impression as to why Uber was willing to pay him—which was never communicated to Sullivan—has nothing to do with the charges against Sullivan,” and should therefore be excluded under Federal Rules of Evidence 401 and 402, along with *Graham*. *Id.* at 15:2-12; *see also* Fed. R. Evid. 402 (“Irrelevant evidence is not admissible.”).

I agree. It is Sullivan’s state of mind that matters, not Glover’s impression of why Uber responded the way that it did or intent regarding the 2016 Incident. There is no suggestion that this impression was communicated to Sullivan himself—the caveat noted in *Graham*. Glover may testify to how Uber’s conduct differed from other companies he dealt with in similar negotiations but his subjective impression is irrelevant and inadmissible.

D. No. 4: Testimony or evidence concerning any of the hackers’ other allegedly criminal activity, including, for example, their participation in other bug bounty programs or other cybersecurity incidents

Both of the hackers’ plea agreements discuss their alleged attempt to extort another company, LinkedIn, by obtaining user account information from Lynda.com, LLC, which is owned by LinkedIn. *See* Mot. in Limine, Angeli Decl., Ex. 2 at 5:16-6:9; Ex. 3 at 5:18-6:12. Sullivan moves to exclude evidence of this and other allegedly criminal activity by the hackers, arguing that it is not relevant under Rule 401 and would turn the trial into a series of “mini trials,” warranting exclusion under Rule 403. *Id.* at 17:9-24.

The government argues that evidence of the hackers’ contemporaneous hacks and attempted extortion of other companies is relevant because “certain members [of] Uber’s security team”—including one of Sullivan’s direct reports—“were aware of some of this conduct” during their response to the 2016 Incident. *Oppo. to Mot. in Limine* at 11:19-12:2. It contends that this evidence is relevant to Sullivan’s state of mind, specifically whether he believed the hackers did

1 not understand how to properly participate in a bug bounty program or were instead engaged in
2 criminal behavior. *Id.* at 12:2-9.

3 Sullivan's state of mind is central to this case. The critical question is whether *Sullivan*
4 knew about the hackers' other allegedly criminal activity during the 2016 Incident at Uber. If the
5 aforementioned members of Uber's security team told Sullivan about the hacks on other
6 companies or he was otherwise aware of them, then the evidence of the hackers' other allegedly
7 criminal activity at the time of the 2016 Incident would be relevant to Sullivan's state of mind. If
8 not, the evidence would not be relevant.

9 At the pretrial conference, the government stated that it had evidence that it believes
10 suggested that Sullivan knew about the other hacks, including notes from his interviews with
11 WilmerHale and an email from his direct report. Rather than issue a blanket prohibition on
12 evidence of the hackers' other allegedly criminal activity, I will wait until the government presents
13 evidence that makes the requisite connection between what members of Uber's security team
14 knew about the contemporaneous hacks and what, if anything, Sullivan knew about them. If that
15 connection is made, evidence related to those other hacks or allegedly criminal activity by the
16 hackers may be admitted. If not, it will be excluded.

17 **E. No. 5: Testimony or evidence relating to the person identified as "Individual**
18 **One" in the hackers' plea agreements, including any testimony or evidence to**
19 **the effect that Individual One had a copy of the Uber data at the heart of the**
20 **2016 Incident**

21 The hackers' plea agreements also indicate that a third person (described only as
22 "Individual One") was involved in the 2016 Incident and obtained a copy of the archive file
23 containing Uber's records. Mot. in Limine, Angeli Decl., Ex. 2 at 5:7-15; Ex. 3 at 5:9-17. The
24 agreements state that the hackers requested that Individual One delete his copy of the data, "which
25 he said he would do," but that the hackers could not confirm that he in fact did so. *See id.* Both
26 hackers also stated in their agreements that they never disclosed to Uber Individual One's
27 involvement in the 2016 Incident. *Id.*

28 Sullivan argues that any testimony or evidence related to Individual One should be
excluded as irrelevant, again because Sullivan's state of mind is key and, as the hackers stated in

the plea agreements, they never disclosed to Uber the fact that Individual One was involved. Mot. in Limine at 19:18-20:2. He further contends that this evidence is irrelevant because “[t]he ultimate fate of the Uber data at the heart of the 2016 Incident has no legal bearing on any of the offenses with which Sullivan is charged.” *Id.* at 20:14-15. He notes that neither section 1505 nor section 4 “requires the government to prove that any particular harm resulted” from his alleged actions. *See id.* at 20:14-22.

In response, the government asserts that this evidence would be relevant to Sullivan’s state of mind should he assert that he reasonably believed that he had secured the data stolen in the 2016 Incident. Oppo. to Mot. in Limine at 12:16-21. If Sullivan makes this argument, the government contends, it should be permitted to present evidence that any such belief “could not have been held in good faith and in reality was completely implausible,” as shown by the involvement of Individual One. *Id.* at 12:19-22.

If the argument is that Sullivan in fact secured the data, then Individual One’s involvement would be relevant, as it would tend to make that consequential fact more or less probable. *See* Fed. R. Evid. 401. But if the argument is that Sullivan *thought* that he secured the data, then it is hard to see how evidence of an undisclosed third hacker is probative of that state of mind. This issue will be decided in the context of the evidence at trial.

II. MOTIONS TO EXCLUDE EXPERT TESTIMONY

Both Sullivan and the government move to exclude proposed testimony by the other’s expert witness. Sullivan seeks to bar portions of the testimony of Daniel Garrie, while the government moves to exclude the entirety of the testimony of James Routh. Dkt. Nos. 138, 139. Their testimony primarily focuses on cybersecurity practices and “bug bounty” programs, where hackers are “rewarded for finding and reporting vulnerabilities” in companies’ cybersecurity systems. *See* Sullivan Mot. to Exclude (“Sullivan Mot.”) [Dkt. No. 138] 1 n.2. (describing bug bounty programs).

Federal Rule of Evidence 702 allows an expert witness qualified “by knowledge, skill, experience, training, or education” to testify “in the form of an opinion or otherwise if:

- (a) the expert’s scientific, technical, or other specialized knowledge will help the

trier of fact to understand the evidence or to determinate a fact in issue;

(b) the testimony is based on sufficient facts or data;

(c) the testimony is the product of reliable principles and methods; and

(d) the expert has reliably applied the principles and methods to the facts of the case.”

Expert testimony is admissible under Rule 702 if it is both relevant and reliable, as shown by the proponent by a preponderance of the evidence. *See Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 589 (1993); *Zeiger v. WellPet LLC*, 526 F. Supp. 3d 652, 667 (N.D. Cal. 2021). Evidence is relevant if it assists the trier of fact in understanding or determining a fact in issue. *Cooper v. Brown*, 510 F.3d 870, 942 (9th Cir. 2007).

For evidence to be reliable, the expert testimony must have “a reliable basis in the knowledge and experience of the relevant discipline.” *Primiano v. Cook*, 598 F.3d 558, 565 (9th Cir. 2010). “The focus of the reliability inquiry is on the principles and methodology an expert uses in forming the opinions rather than the expert’s conclusions.” *In re Viagra (Sildenafil Citrate) & Cialis (Tadalafil) Prod. Liab. Litig.*, 424 F. Supp. 3d 781, 790 (N.D. Cal. Jan. 13, 2020). The ultimate question is whether the proponent can “establish the reliability of the principles and methods employed to draw a conclusion regarding the particular matter to which the expert testimony was directly relevant.” *United States v. Hermanek*, 289 F.3d 1076, 1094 (9th Cir. 2002) (citation and quotation marks omitted).

Although *Daubert* proffers “several reliability factors,” the reliability inquiry is flexible, giving the district court broad latitude to determine the appropriate form of inquiry. *United States v. Valencia-Lopez*, 971 F.3d 891, 898 (9th Cir. 2020) (citations omitted). The Ninth Circuit has acknowledged that *Daubert* “may be harder to apply when the expert testimony is ‘experience-based’ rather than ‘science-based.’” *Id.* “But any such difficulty cannot simply lead to a ‘that goes to weight, not admissibility’ default.” *Id.*

A note to Rule 702 offers some additional guidance: “If the witness is relying solely or primarily on experience, then the witness must explain how that experience leads to the conclusion reached, why that experience is a sufficient basis for the opinion, and how that experience is

1 reliably applied to the facts.” Fed. R. Evid. 702 advisory committee note (2000).

2 The Ninth Circuit has emphasized *Daubert*’s guidance that Rule 702 “should be applied
3 with a ‘liberal thrust’ favoring admission.” *Messick v. Novartis Pharm. Corp.*, 747 F.3d 1193,
4 1196 (9th Cir. 2014) (citing *Daubert*, 509 U.S. at 588). “Shaky but admissible evidence is to be
5 attacked by cross examination, contrary evidence, and attention to the burden of proof, not
6 exclusion.” *Primiano*, 598 F.3d at 564.

7 **A. Sullivan’s Motion to Exclude Garrie’s Testimony**

8 Sullivan moves to exclude Garrie’s proposed testimony about: (1) bug bounty programs;
9 (2) Sullivan’s deposition with the FTC; (3) any “ransom” involved in the 2016 Incident; (4) legal
10 opinions about how the 2016 Incident was handled; and (5) Sullivan’s state of mind. Sullivan
11 Mot. at i-iii. The motion is largely DENIED. Garrie is qualified to testify as an expert and may
12 testify to all of these matters except any legal conclusion that California’s disclosure law was
13 violated or the legal status of the hackers as agents or employees of Uber. He also may not testify
14 whether Sullivan acted “intentionally” or “intended” to do anything, though he may state the facts
15 underlying his conclusions and respond to hypothetical scenarios. Otherwise, Garrie’s opinions at
16 issue may come in, for reasons explained in further detail below.

17 **1. Bug Bounty Testimony**

18 Sullivan first challenges Garrie’s qualifications, arguing that the government has not
19 shown that Garrie has sufficient experience with bug bounty programs to qualify him as an expert.
20 *Id.* at 8:15-9:9. In addition, he contends that Garrie’s testimony only rehashes the government’s
21 version of the facts and is therefore not helpful to the trier of fact, as required by Rule 702(a). *Id.*
22 at 10:14-11:5. Finally, he argues that Garrie’s testimony about bug bounties should be excluded
23 because the government failed to establish its reliability. *Id.* at 11:22-25.

24 None of these points are convincing. The government has met its burden in showing that
25 Garrie is qualified to testify about bug bounty programs. He has extensive professional experience
26 in cybersecurity, co-founding a cybersecurity and forensic engineering firm, teaching
27 cybersecurity classes and trainings, publishing books and articles on cybersecurity, and serving as
28 an expert witness on cybersecurity. *See* Oppo. to Sullivan Mot. [Dkt. No. 152] Ex. 1 at 1. He also

has specific experience related to bug bounties. The supplemental resume submitted by the government shows this. Garrie has consulted companies on the establishment and operation of bug bounty programs since 2016. *Id.* at 15. As part of that work, he has analyzed and reviewed bug bounty programs, and advised companies on the “consequences of poorly designed or executed” programs. *Id.* This professional experience qualifies him to offer testimony that Sullivan’s alleged actions “were not consistent with industry best practices or Uber’s bug bounty program.” *See* Sullivan Mot., Angeli Decl., Ex. 1 at 10 (summarizing Garrie’s proposed testimony).

The government has also shown that Garrie’s testimony is reliable. It underscores Garrie’s experience “evaluating, designing, and implementing bug bounty programs” and the specific facts he relied upon in opining that Sullivan’s actions regarding the 2016 Incident were inconsistent with industry best practices. *Oppo. to Sullivan Mot.* at 4:4-25. Unlike in *Hermanek*, where the court excluded testimony because the expert “failed to explain in any detail the knowledge, investigatory facts and evidence he was drawing from,” the government has identified in detail that knowledge and those facts. *See* 289 F.3d at 1094. The summary of Garrie’s testimony compares facts alleged in this case with “standard bug bounty practice,” further showing how Garrie applied his experience to the facts. *See* Sullivan Mot., Angeli Decl., Ex. 1 at 10-11. Nor does it appear that Garrie’s testimony will simply regurgitate the government’s version of events. The side-by-side comparison of alleged facts and industry best practices indicate that Garrie’s testimony will help the jury understand the evidence or determine a fact in issue.

Sullivan’s motion to exclude Garrie’s testimony on bug bounty programs is DENIED.

2. Testimony About Sullivan’s FTC Deposition

Next, Sullivan moves to exclude Garrie’s testimony about Sullivan’s deposition to the FTC under Rules 401, 402, and 403. *Id.* at 12:18-13:7. That testimony is summarized as:

Sullivan’s FTC deposition included various declarative statements regarding Uber-specific cybersecurity controls (e.g., encryption and key management) that the 2016 breach later revealed were incorrect, including encryption and key management. (see generally Mandiant report, preacher tracker, etc.)

Id. (citing Angeli Decl., Ex. 1 at 12). Sullivan argues that this testimony is irrelevant and “would

likely confuse the jury about the issues before it,” as he is “not charged with failing to correct his testimony concerning Uber’s cybersecurity controls, but instead with affirmatively concealing the 2016 Incident.” *Id.* at 12:21-24.

The government asserts that Sullivan told the FTC that “Uber had improved its cybersecurity and fixed the problems” that led to a previous data breach in 2014. *Oppo.* to Sullivan Mot. at 5:17-18. According to the government, 10 days after his deposition, Sullivan learned that Uber had again been hacked and that many of his statements “were either not true, misleading, or misleadingly incomplete.” *Id.* at 5:18-20.

Garrie’s opinion that Sullivan’s statements were later shown to be incorrect speaks to Sullivan’s motive for concealing the 2016 Incident from the FTC. The government argues that the evidence will show that Sullivan referenced his “previous assertions” in Uber’s contemporaneous record of the breach response. *See id.* at 5:21-27. That motive is of consequence—to convict Sullivan of the obstruction charge, the government must prove beyond a reasonable doubt that he “intentionally endeavored corruptly” to influence, obstruct, or impede the FTC proceeding. *See Price*, 951 F.2d at 1031. Garrie’s testimony also has a tendency to make it more or less probable that Sullivan obstructed the FTC by failing or causing others to fail to correct any information previously provided to the FTC. This portion of Garrie’s testimony is therefore relevant under Rule 401.

Any risk that this testimony will confuse the jury about the issues is not substantially outweighed by the testimony’s probative value, as required for exclusion under Rule 403. Moreover, any such risk can be addressed through the jury instructions, which will state the two crimes that Sullivan faces and the elements of each.

Sullivan’s motion to exclude Garrie’s testimony about his FTC deposition is DENIED.

3. Testimony Describing the 2016 Incident as “Ransom”

Third, Sullivan seeks to exclude Garrie’s characterizations of the 2016 Incident as a “ransom” or “ransom-type situation” under Rules 403 and 702. Sullivan Mot. at I, 13:8-14:16. Specifically, he moves to exclude the following characterizations:

- “. . . when responding to a significant incident, such as a ransom-type

situation.”

- “Correspondence with the hacker plays out like ransom negotiation rather than bug bounty”
- “. . . industry best practices for a CSO responding to a data breach, especially one involving a ransom . . .”
- “Discussion of consequences that would occur if companies were allowed to bar hackers from disclosing data breaches and ransom payments by having hackers sign NDAs or by classifying the hackers as agents or employees of the company.”

Id. at i (citing Angeli Decl., Ex. 1 at 7, 9, 11-12).

Sullivan argues that the terms “ransom” or “ransom-type situation” have no probative value, as “the jury is capable of listening to the facts concerning the 2016 Incident and drawing its own conclusions as to their meaning.” *Id.* at 13:19-23. Moreover, he contends, the word “ransom,” used by an expert witness, would be “unfairly inflammatory.” *Id.* at 13:23-24. In support, he points to a Northern District of California case where the court, citing Rule 403, precluded an expert witness from offering “inflammatory characterizations” of the defendants’ conduct, “including terms such as ‘pummeled,’ ‘beating the dickens out of,’ and ‘beat into submission.’” *Id.* (citing *Cotton v. City of Eureka*, No. C-08-04386-SBA, 2010 WL 5154945, at *14 (N.D. Cal. Dec. 14, 2010)). Similarly, Sullivan argues, this testimony should be excluded under Rule 403.

The word “ransom” has an ordinary usage that is not limited to the cybersecurity context. It appears from the cited portions of Garrie’s summary that he uses “ransom” or “ransom-type situation” to describe the hackers’ actions or industry best practices for responding to similar actions, both of which would help the jury to understand the evidence or to determine a fact at issue under Rule 702. It also appears that he uses this term in a way that a lay person would understand it to be used—to describe “a consideration paid or demanded for the release of someone or something from captivity.” *See* Merriam-Webster Online Dictionary, “Ransom,” <https://www.merriam-webster.com/dictionary/ransom> (last accessed Aug. 24, 2022). The ordinary use of a word to describe a situation is a far cry from the language excluded in *Cotton*, where the expert was precluded from characterizing police officers’ conduct using terms as “pummeled,”

“beating the dickens out of,” and “beat into submission.” *See* 2010 WL 5154945, at *14.

Sullivan’s motion is DENIED regarding this aspect of Garrie’s proposed testimony.

4. Opinions About How the 2016 Incident was Handled

Sullivan also moves to exclude what he describes as improper legal conclusions by Garrie:

- “Once a hacker obtains such access to data, they should not proceed with access and should notify the company. They would then contact a legal specialist to assess the situation further.”
- “Accordingly, Sullivan was still responsible for communications with the A-Team in regards to the status of the incident.”
- “Sullivan’s decision to not report or disclose the incident to the CA Attorney General and/or the Uber drivers violated various California notification and disclosure laws . . .”
- “Rice at 9: ‘seemed like extortion to them [HackerOne] because the hacker had vulnerability information and would not release information about it without getting paid.’”
- “Sullivan’s decision to require the Hackers to sign the non-disclosure agreement (‘NDA’) does not make the Hackers employees or agents of Uber under any law or statute.”

Sullivan Mot. at ii (citing Angeli Decl., Ex. 1 at 8, 10-12).

An expert witness “cannot give an opinion as to her legal conclusion, i.e., an opinion on an ultimate issue of law.” *Nationwide Transp. Fin. v. Cass Info. Sys., Inc.*, 523 F.3d 1051, 1058 (9th Cir. 2008). “District courts may, accordingly, preclude witnesses from relating legal conclusions, but not the facts underpinning those conclusions (so long as they are otherwise admissible).” *Zeiger*, 526 F. Supp. 3d at 680 (citation omitted).

Two of the referenced statements—that Sullivan’s decision not to report or disclose the incident violated California law, and that his decision to require the hackers to sign the NDA did not lawfully make the hackers Uber’s employees or agents—are clearly legal conclusions and therefore inadmissible.

The context of the remaining statements indicate that they do not amount to legal conclusions. Garrie’s proposed testimony about what a hacker “should” or “should not” do after accessing a company’s data speaks to how bug bounties generally operate. *See* Sullivan Mot.,

1 Angeli Decl., Ex. 1 at 8. His testimony about Sullivan’s responsibilities offers an opinion based
 2 on his review of the evidence in the case. *See id.* at 9-10. The same is true of his proposed
 3 testimony regarding the hackers’ possession of information and willingness to release it. *See id.* at
 4 5. There is no legal advice hidden within, as Sullivan asserts, let alone any legal conclusion. *See*
 5 *id.* at 15:15-21.

6 This motion is GRANTED in part and DENIED in part. Garrie’s testimony that Sullivan
 7 violated California disclosure law and that his decision to have the hackers sign the NDA did not
 8 lawfully make them employees or agents of Uber amount to legal conclusions and are excluded.
 9 The remaining statements are admissible.

10 **5. Testimony About Sullivan’s State of Mind**

11 Finally, Sullivan moves to exclude testimony by Garrie regarding Sullivan’s knowledge,
 12 intent, and state of mind under Rules 702 and 704(b). He points to 14 statements pulled from
 13 Garrie’s proposed testimony that he argues constitute opinions regarding Sullivan’s mental state.
 14 *Id.* at ii-iii (listing each statement), 16:12-18. The contested statements range from testimony that
 15 Sullivan “knew” about the 2016 Incident and the type of information exposed, to that he acted
 16 “intentionally” in certain circumstances, and that he “could not, in good faith, have thought that
 17 this breach did not need to be reported.” *Id.* at 16:12-18

18 Rule 704(b) plainly prohibits an expert witness in a criminal case from stating an opinion
 19 “about whether the defendant did or did not have a mental state or condition that constitutes an
 20 element of the crime charged or of a defense.” Fed. R. Evid. 704(b). As the Rule states: “Those
 21 matters are for the trier of fact alone.” *Id.*

22 The government agrees that Garrie cannot offer opinion testimony that Sullivan “knew or
 23 understood a particular fact or had a particular state of mind at a particular time.” *Oppo.* to
 24 Sullivan Mot. at 8:8-12. It does not oppose excluding such opinions. *Id.* However, it argues,
 25 Garrie *can* rely on evidence that Sullivan “knew certain things or said or did certain things that
 26 provide the basis for” Garrie’s testimony.” *Id.*

27 Some of the testimony cited by Sullivan is clearly barred by Rule 704(b). This includes
 28 any statements that Sullivan acted “intentionally” or made an “intentional” decision. Garrie can,

1 however, state the relevant facts underlying his conclusions and respond to hypothetical scenarios.
2 To the extent that his testimony strays from these guideposts, I will consider specific objections at
3 the time they are raised during trial.

4 **B. The Government’s Motion to Exclude Routh’s Testimony**

5 The government moves to exclude Routh’s testimony. Gov’t Mot. to Exclude (“Gov’t
6 Mot.”) [Dkt. No. 139] 1. This motion is DENIED.

7 The government first attacks the reliability of Routh’s testimony, arguing that it is not clear
8 what “reliable principles and methods” he used beyond his personal experience in drawing his
9 conclusions, nor how his experience with cybersecurity at financial services companies serves as a
10 basis for cybersecurity practices at a tech company like Uber. *Id.* at 3:24-4:8. It next contends
11 that Routh’s testimony should be excluded because it is “common sense and undisputed” and,
12 borrowing an earlier argument from Sullivan, would merely parrot the testimony of lay witnesses.
13 *See id.* at 6:10-20. Finally, the government argues that because the case “turns almost entirely on
14 defendant’s state of mind” related to the 2016 Incident, Routh’s “generalized opinions about what
15 other companies may or may not have done should be excluded as irrelevant as to what Uber
16 employees actually believed in 2016 and 2017.” *Id.* at 6:22-7:17.

17 The primary issue is whether Sullivan has shown that Routh’s proposed testimony is
18 reliable. Routh is qualified to testify as an expert witness based on his experience; he led
19 cybersecurity efforts at several large companies over the last 20 years, sits on several
20 cybersecurity boards, teaches sessions on cybersecurity practices, and advises cybersecurity
21 groups. *See* Gov’t Mot., Ex. 1 at 6-7. At the pretrial conference, counsel for Sullivan sufficiently
22 drew the link between Routh’s experience and his proffered conclusions about hacker
23 communications and bug bounty programs, noting that he has personal involvement in bug bounty
24 programs, has led cross-company and cross-sector organizations that advice cybersecurity
25 practices, and that as part of his work, shared intelligence about hackers with other cybersecurity
26 officials in order to prevent harm to other companies. This is enough to satisfy *Hermanek* and
27 establish the reliability of Routh’s proposed testimony.

28 The government’s remaining arguments also fall short. Routh’s proposed testimony does

more than state undisputed facts or reiterate the testimony of lay witnesses. Rather, it includes descriptions of different hackers and how they “fit into cybersecurity and bug bounty programs”; how companies discern when to report cybersecurity incidents to law enforcement; and how bug bounty programs help companies learn about the effectiveness of their cybersecurity controls. *Id.* at 2-4 (summarizing Routh’s proposed testimony). This testimony will help the jury understand the evidence or determine facts at issue as required by Rule 702, particularly given the technical nature of cybersecurity and bug bounty programs that might not be readily obvious to a layperson.

Routh’s proposed testimony will also show how companies used bug bounty programs and responded to cybersecurity incidents during the relevant time period. *Id.* at 1-4. As Sullivan notes, whether his actions aligned with industry standards tends to make it more or less probable that he had the requisite intent. *See* Oppo. to Gov’t Mot. [Dkt. No. 153] 8:9-23. Like Garrie, Routh’s proposed testimony includes his opinion on whether “the actions of Uber’s security team during the 2016 Incident were consistent with” industry standards. *See* Gov’t Mot., Ex. 1 at 3. Routh’s testimony is just as relevant as Garrie’s under Rule 401.

III. OBJECTIONS TO EXHIBITS

Finally, both parties object to various exhibits listed by the opposing side. Dkt. Nos. 146, 148. I gave my general reactions to the descriptions of the exhibits but I have not seen them. Whether the disputed evidence is admissible will depend on how it is proffered at trial. I will make those decisions on a case-by-case basis, as the objections are raised at trial and much-needed context is provided to determine whether the exhibits are in fact admissible.

I have ordered that records relating to Sullivan’s third interview with Uber be produced to the government, which Uber has agreed to provide. Additionally, the parties shall meet and confer regarding how the interview documents will be handled. These documents appear to be admissible, not for the truth of the matter asserted, but for the fact of disclosure. I will reserve judgment on whether they constitute a present sense impression under Federal Rule of Evidence 803(1) or past recollection recorded under Rule 803(5).

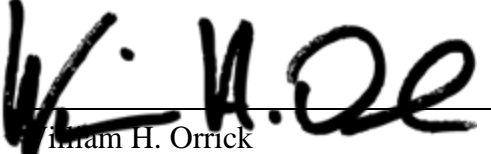
CONCLUSION

Sullivan’s motions in limine are GRANTED in part and DENIED in part, in the manner

described above. The motions to exclude the expert witness testimony are DENIED, except as indicated. I will defer deciding specific evidentiary objections until they are raised at trial.

IT IS SO ORDERED.

Dated: August 27, 2022


William H. Orrick
United States District Judge

United States District Court
Northern District of California